Non-IT Y2K Contingency Plans

A Guide for USDA Buildings

JUNE 1999

INTRODUCTION

At the turn of the century, equipment with clock or date functionality may malfunction or shut down unless it has a four-digit year-dating system. The use of only two digits—for example, "03" to denote 2003—may result in the storing of the incorrect date (e.g., 1903 rather than 2003) or in the loss of date- and time-specific controls, which will in turn cause arithmetic errors in computations and problems in the sorting of calendar-year data.

While information technology (IT) systems receive most of the publicity about the impact of year 2000 (Y2K), non-IT equipment also will be affected. Examples of such equipment are energy management control systems that automatically shut down heating, ventilation, and air conditioning systems after normal business hours; building access control systems that are calendar date sensitive; and security system devices that record the date and time on tape.

Government agencies have undertaken a massive effort to bring their non-IT equipment into Y2K compliance. The U.S. Department of Agriculture (USDA) is no exception. Over the last 14 months, the USDA has implemented a program designed to minimize the likelihood of Y2K-related failures occurring in its non-IT building infrastructure systems at the turn of the century. To date, the following steps have been, or in the progress of being, completed throughout the nation:

Identified non-IT building infrastructure components that may be potentially impacted by a Y2K.

Identified the non-IT building infrastructure systems that are mission critical and Y2K susceptible.

Contacted vendors to determine whether the inventoried building systems with clock or date functions are Y2K compliant.

Tested mission-critical, Y2K-susceptible, non-IT building systems thought to be compliant or whose compliance was not known.

Renovated—repaired or replaced—equipment identified through vendor information and field testing as noncompliant.

While USDA is taking every precaution to ensure that all of its non-IT building systems are Y2K ready, it is still possible that some equipment will malfunction at the turn of the century. Any equipment failures will, at a minimum, disrupt business-as-usual.

USDA must decide *now* how it will mitigate the effects of any Y2K-related failures of mission-critical devices. This guide specifies what you need to do to prepare for such equipment failures. It describes phases of contingency plans and specifies steps that you need to take to implement contingency operations

BUILDING SYSTEMS REQUIRING A CONTINGENCY PLAN

A building-specific Y2K contingency plan should be prepared for each building with systems potentially impacted by Y2K. At a minimum, the contingency plan should cover

all USDA-owned, mission-critical, non-IT building systems with a clock or date function,

all USDA-leased buildings with mission-critical, non-IT building systems, and

support services provided to USDA whose failure would significantly affect the life and safety of federal employees or the building's operations (e.g., utilities).

USDA-Owned Buildings

Contingency plans should be developed for all USDA-owned equipment, including those that have

passed Y2K field tests,

been declared to be Y2K compliant by the vendor, and

been renovated so that it is now Y2K compliant.

The following building systems have been determined to be mission critical:[1]

access control system

[1] Mission-critical components/systems are defined as those components that should a failure or malfunction occur could pose life and safety hazard or significantly impact building operations. The final determination of which systems in a particular building are deemed "mission critical" should be accomplished at a local level, taking into consideration local conditions. For example, in January, a heating system may be "mission critical" in Omaha, Nebraska, but not Orlando, Florida.

boiler/water heater

chiller

CO-level monitor

electrical plant

emergency lighting

energy-management-control systems

fire alarm system

fire sprinkler system

generator

halon release system

heating, ventilation, and air-conditioning (HVAC)

interior lighting (automatic)

passenger elevators

power distribution unit

programmable thermostat

security system

uninterruptible power supply (UPS).

USDA-Leased Buildings

USDA should identify a USDA point of contact (POC) for each of its leased buildings. This POC should have the name and phone number of the landlord in case the landlord must be contacted. USDA POCs should contact the General Services Administration (GSA) or the commercial landlord and ask to see the building's contingency plan that has been prepared by the landlord, if it exists. In addition, the USDA POC should discuss with the landlord the plans for assessing the building systems' operability during the weekend. Specifically, the USDA POC should determine if the landlord is planning to enter and inspect the building over the weekend or is relying on USDA to make the first operability assessment.

Utilities

Some services, such as power and water, are supplied by local utilities. While we cannot fix these systems should they fail because of a Y2K problem, USDA must have a contingency plan for how it will operate in case a service-provider experiences a Y2K problem that affects them. For example, if power goes out in an office, the contingency plan may be to send workers home and transfer work to other offices around the country (similar to a normal power outage). However, this approach may not be acceptable at all buildings, and backup generators may need to be procured ahead of time.

Note: It is *not* necessary to develop contingency plans for equipment that will be retired by 2000 or for equipment covered by the USDA IT Y2K programs.

CONTINGENCY PLANS—IMPLEMENTATION PHASES

A contingency plan is implemented in three phases: (1) contingency planning—identifying the steps to be taken to ensure that your building is prepared to minimize the impact if the equipment fails; (2) contingency operations—implementing the actions identified in your contingency plans to continue operations if the equipment *does* fail; and (3) postcontingency activities—implementing the actions necessary to return to normal operations.

The following subsections describe the actions your office should take, or be prepared to take, for each phase.

Phase I—Contingency Planning

Contingency plans for building infrastructure systems will focus on providing manual overrides or using encapsulation—having the system use an alternative date as a temporary work-around. Contingency plans will include guidance for equipment work-arounds and the advance preparation necessary to implement a contingency plan once a failure has occurred. Activities include making sure that operational manuals are readily available, having alternative vendor contracts or supplies in place, and identifying the person responsible for resetting the date on the equipment. A critical part of the contingency planning for building infrastructure systems is disseminating the information prior to failure so that advance preparations can be made at the local level. For example, if a security system fails to operate, identification badges may have to be checked manually or guards may have to replace automated intrusion-detection devices, requiring additional USDA or contract personnel on short notice.

The following steps should be provided for each building:

1. *Designate roles, responsibilities, and authorities*. For each building, establish written guidelines for roles, responsibilities, and limits of authority

should a Y2K event disrupt equipment and/or buildings operations. Roles should be established for

a contingency operations manager who is responsible for managing contingency operations for all equipment at each owned building or, in the case of leased buildings, the USDA POC who is responsible for contacting the landlord for building status; and

a Y2K monitor(s) who is responsible for monitoring the specific equipment at the possible failure dates. Note: In smaller buildings the contingency operations manager and the Y2K monitor may be the same person.

Other needed actions are as follows:

Identify procedures and local POCs for emergency notification. Typical POCs may include utility companies, equipment-service representatives for mission-critical systems, agency management, GSA or landlord representatives, and the Y2K Program Office.

2. *Gather product-specific information and develop a failure-monitoring plan for USDA-owned equipment.* The USDA employee who is the Y2K monitor for a particular type of equipment should gather the following information to ensure that he or she is prepared to monitor the equipment during the critical Y2K dates:

Document the names of the manufacturer’s representative and any other service providers for this equipment. Obtain Web-site information for your vendor representative or equipment manufacturer. Ensure a service contract is in place if appropriate. Develop communication protocol with service contractors that specifies all telephone, pager, radio numbers and codes, including night, weekend, and holiday numbers.

Locate all user manuals and drawings and ensure that the Y2K monitor for the equipment is familiar with the contents. Identify components that could fail and develop a plan for monitoring those components. Develop a checklist to determine the number, type, and location of any connected equipment that could in turn affect or be affected by a failure of this equipment.

Determine how operations personnel will access the building, including the entire interior, on January 1, 2000, should an access-control system fail (e.g., a bypass electrical or mechanical locking system may need to be installed in at least one entrance location).

Develop a checklist specifying all inspection procedures needed to ensure full operation of the equipment and any connected systems.

Ensure that the Y2K monitor knows how to start and shut down the equipment. Procedures for complex equipment should be documented. Set the policy for how the Y2K monitor will monitor the equipment on January 1, 2000, and on other critical Y2K dates (e.g., come in ahead of time and test).

The Department strongly recommends that building operations personnel occupy the building on January 1, 2000, to assess the building's condition relative to year 2000 and to identify any applicable contingency-plan items that need to be implemented. In addition, all computer or communications centers should, if possible, shut down at 10:00 p.m. on December 31, 1999, until 6:00 a.m. on January 1, 2000. The shutdown would allow electric utility companies an 8-hour period to provide reliable service without voltage brownouts and blackouts. This time period starts 1 hour before trouble would begin in the eastern time zone and extends past the Alaskan time zone.

3. *Develop operational alternatives for USDA-owned equipment*. A long-term interruption of equipment service or operation caused by a Y2K failure might seriously affect operations of your office. In advance, you must identify alternative methods of using the equipment. Assess the cost and benefits of identified alternatives and select the preferred strategy. Procure additional supplies, if necessary (e.g., in lieu of a boiler, obtain hot water and space heaters and have them on hand prior to the critical Y2K dates). Examples of operational alternatives follow:

   Central fire alarm systems. If the actual operation of the fire alarm system may be compromised (versus historic date stamping), obtain a sufficient supply of battery-operated fire alarms.

   Building access control and general security. Establish a schedule and responsibilities for conducting random checks of each building. Post monitors at public entrances. Assign responsibilities for ensuring that the building is secured at the end of the day.

   Elevators and escalators. Operate the elevator manually using two-way radios.

   HVAC systems. Operate in manual mode.

X-ray systems. Increase the use of alternative invasive inspections, which may require additional contract personnel to be on standby.

UPS systems. Increase the on-site supply of backup batteries.

4. *Establish emergency procedures for contingency operations.* Ensure knowledge of safe date-disabling and date-changing procedures (use manual overrides, change the method of date calculation or representation, disable certain date-sensitive components), if applicable. Verify procedures for notifying building occupants and agency management.

5. *Test emergency procedures.* To ensure that the contingency plan is complete, the contingency operations manager should consider training staff and practicing actions that should be taken if the equipment fails (risk is much higher without a rehearsed contingency plan). During rehearsal, document the procedures that should be followed before, during, and after the failure dates.

6. *Develop a postcontingency plan.* Develop a plan for returning equipment that has failed to normal operation. This plan should cover required postrepair equipment testing, cancellation of contingency-support agreements, return of leased contingency equipment, and notification of authorities of problem resolution.

Phase II—Contingency Operations

The contingency operations phase involves activating the contingency plans. Beginning immediately, your office needs to take the following steps if the equipment fails:

1. Review contingency plans and execute them where necessary.

2. Identify recovery alternatives. Determine if malfunctioning equipment can be temporarily fixed (i.e., reset clock using a pre-2000 alternative date), or manually operated. If the equipment cannot be temporarily repaired or manually operated, identify the most cost-effective corrective action.

3. Notify the appropriate authorities of the nature and scope of the Y2K problem and of the intended solution.

4. Temporarily fix, manually operate, procure, repair, or replace where applicable.

5. Monitor the equipment to ensure that the “corrective actions” are adequate.

Phase III—Postcontingency Activities

After a failure occurs and your office has taken the necessary steps to recover from the failure, you must then return operations to normal. Postcontingency activities are as follows:

1. Identify the most cost-effective, long-term alternative, if the equipment or process used in the alternative operations will not support a long-term solution.

2. Test the “corrected” equipment functions and review the results.

3. Notify the appropriate authorities.

DIRECTIONS FOR IMPLEMENTATION

The first step in your contingency planning is to assign responsibility for contingency monitoring and management. Next, identify all of the USDA-owned, mission-critical, non-IT equipment with date or clock functionality for which a contingency plan must be implemented at your location. Identify the landlord POCs for leased buildings.

Next, make a copy of the *Building-Specific Y2K Contingency Planning Checklist* (see Appendix). One form should be completed for each USDA-owned building. Typically, the USDA contingency operations manager should oversee the development of the building-specific Y2K contingency plan. Contact landlords in leased buildings to discuss monitoring activities.

Finally, we recommend that your building’s occupants be made aware of the existence of the building-specific Y2K contingency plan. However, for security purposes, distribution of the contingency plans should be limited to those who are actually involved in the contingency plan execution.